UNIVERZA V LJUBLJANI
FAKULTETA ZA ELEKTROTEHNIKO

SEMINARSKA NALOGA
PRI PREDMETU MOBILNE KOMUNIKACIJE

IPv6 V OMREŽJIH GPRS IN UMTS

Rudolf Sušnik

Mentor: prof. dr. Sašo Tomažič

LJUBLJANA, avgust 2002

KAZALO

1. UVOD

Dve izmed najhitreje razvijajočih se področij v telekomunikacijah internet in mobilna omrežja. V stacionarnih omrežjih je internet že globoko zasidran, še večji vpliv pa utegne dobiti z razvojem v smeri mobilnosti – mobilnost v internetu in mobilni internet. Kadar govorimo o mobilnosti se nam pojavi asociacija z mobilnimi omrežji (npr. GSM, GPRS, UMTS) in v tej smeri je uporaba interneta v mobilnih aplikacijah tudi popularizacija mobilnih komunikacij.

Danes večina internetskih omrežij deluje po protokolu IPv4 (Internet Protocol Version 4), ki počasi dosega meje lastnih omejitev. Glavni problem je predvsem obseg naslovnega prostora, poleg tega pa tudi zagotavljanje varnosti in podpora kvaliteti storitev. Za reševanje teh problemov je predviden IPv6 – internetni protokol naslednje generacije. S tem protokolom ne bodo rešeni vsi problemi, bo pa zagotovo rešen problem naslovnega prostora, saj je v IPv6 možnih kar 2^{128} ali 10^{38} različnih naslovov.

Poleg omejenosti naslovnega prostora v IPv4 (ob sedanjih trendih je pričakovati, da bodo naslovi pošli okoli l. 2004) je težava v neenakomerni geografski razporeditvi naslovov. Azija, kot potencialno največji trg mobilne telefonije, ima v IPv4 izredno majhen naslovni prostor in zato ne preseneča, da so prav Azijci med pospeševalci uvajanja IPv6.

Z uvajanjem mobilnih storitev (storitve WAP, prenosni računalniki s podatkovno povezavo) se povečuje potreba po naslovih IP. V okoljih IPv4 se problemu delno izognemo z uporabo zasebnih naslovov, tuneliranja ter prevajanja (NAT – Network Address Translation). Tak pristop je le izhod v sili, zato je rešitev v obliki IPv6 nujna.

Prehod iz IPv4 v IPv6 poteka in bo potekal postopoma, pri čemer se uporabljajo različne rešitve. V seminarski nalogi si bomo ogledali protokole za paketni prenos podatkov v omrežjih GPRS (General Packet Radio System) in UMTS (Universal Mobile Telecommunications Service), mobilnost v IPv6, predviden prehod omrežij s protokola IPv4 v protokol IPv6 ter delovanje protokola IPv6 v množici različnih dostopovnih tehnologij omrežij 3G in 4G.

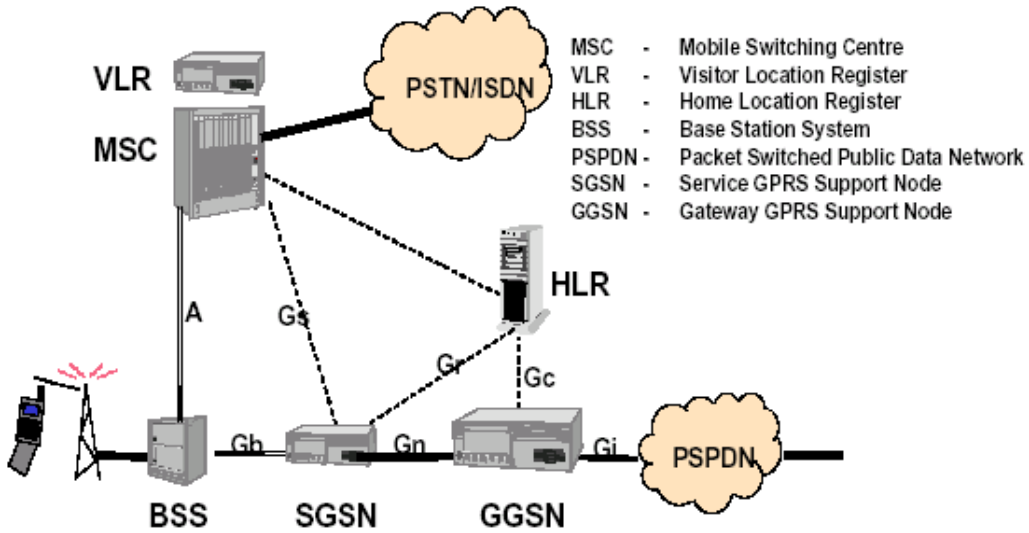
2. PAKETNI PRENOS PODATKOV V GPRS IN UMTS

S stališča protokola IP, ki na omrežnem nivoju zagotavlja povezovanje končnih naprav, razlik med omrežjema GPRS in UMTS ni. Edina razlika, ki jo lahko občuti uporabnik je hitrost prenosa podatkov, ki je posledica različnosti radijskih vmesnikov. Slednje je tudi bistvena razlika med obema sistemoma, kar bo podrobneje prikazano v naslednjih poglavjih, za našo obravnavo prenosa uporabniških podatkov pa je vseeno ali govorimo o omrežju GPRS ali UMTS.

2. 1. ZGRADBA OMREŽJA GPRS

Omrežje GPRS je zgrajeno kot razširitev sistema GSM (Global System for Mobile communications) za nepovezavno orientirane storitve prenosa paketnih podatkov. V ta namen je omrežju dodanih nekaj novih elementov med katerimi sta glavnega pomena vozlišči SGSN (Serving GPRS Support Node – strežno podporno vozlišče GPRS) in GGSN (Gateway GPRS Support Node – prehodno podporno vozlišče GPRS). Kontrolerju baznih postaj BSC (Base Station Controller) je dodana paketna krmilna enota PCU (Packet Control Unit), ki skrbi za dodeljevanje zmogljivost radijske povezave.

Strežno podporno vozlišče GPRS nadzoruje stanje mobilne postaje in sledi njenim premikom. Poleg tega je vozlišče SGSN služi za vzpostavitev in nadzorovanje podatkovne povezave med mobilnim terminalom in ciljnim omrežjem.

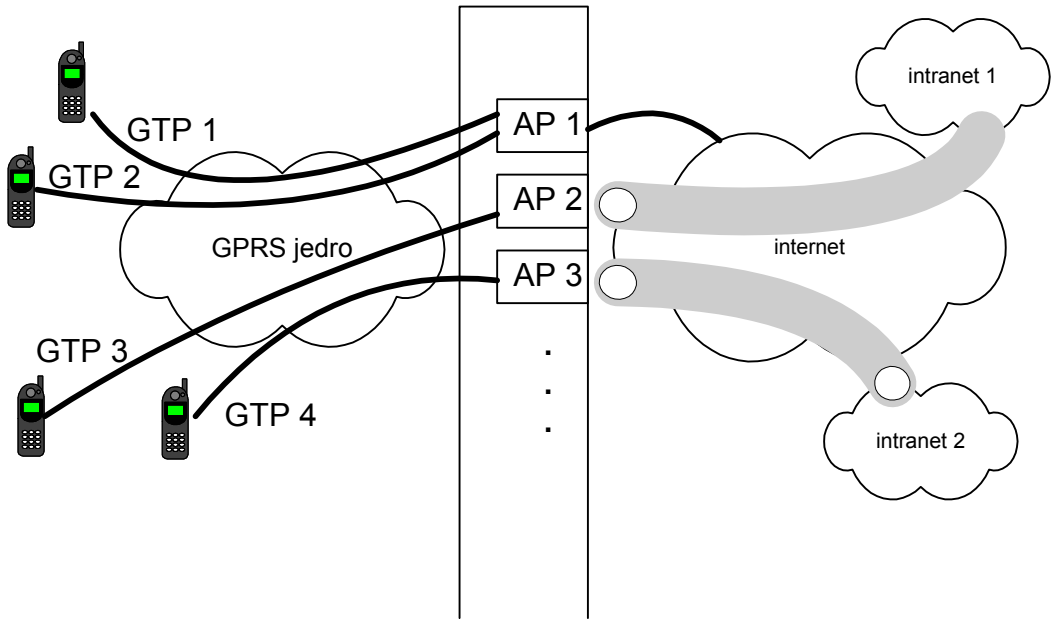


slika 1: omrežje GPRS

Prehodno podporno vozlišče GPRS predstavlja prehod med omrežjem mobilnega operaterja in zunanjim podatkovnim omrežjem kot je to npr. internet. Za prehod uporabniških paketov v zunanje paketno omrežje je ključnega pomena dostopovna točka (AP – Access Point). Vozlišče GGSN si lahko zamišljamo kot skupek dostopovnih točk, ki se ločijo po imenih.

Mobilna naprava naslavlja dostopovno točko z njenim imenom – ime dostopovne točke, APN (Access Point Name), zato večkrat govorimo o »APN-jih« namesto o »AP-jih«.

Vsak mobilni terminal mora vedeti s katero dostopovno točko naj komunicira, kar mu določimo ob vzpostavitvi zveze. Vsaka dostopovna točka ponuja povezovanje v določeno omrežje, tako imamo npr. AP za neposredni prehod v internet, AP za dostop do nekega intraneta skozi tunel ipd. Za lažjo predstavo dostopovnih točk služi slika 2.

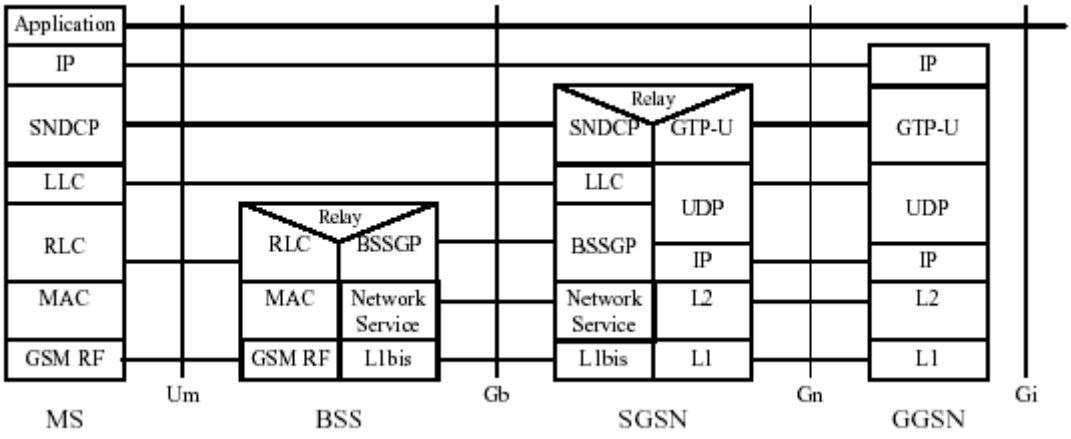


slika 2: dostopovne točke

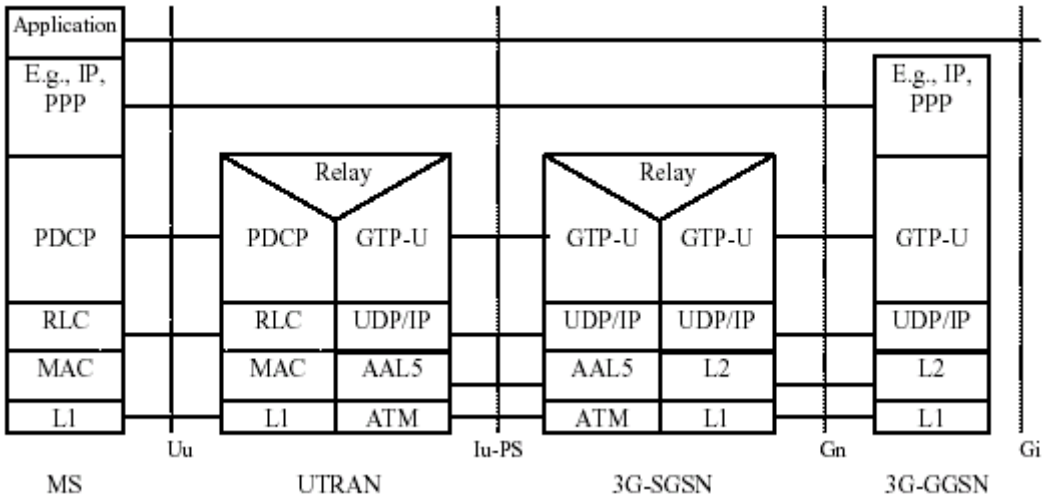
Za paketni prenos podatkov, ki poteka med mobilnim terminalom in zunanjim paketnim omrežjem (PSPDN), so bistvenega pomena predvsem vmesniki Um, Abis, Gb, Gn in Gi po katerih poteka prenos paketov. Podrobnejšo obdelavo zaslužijo zadnji trije, ki predstavljajo novost v primerjavi z GSM.

2. 2. PROTOKOLNI SKLADI V GPRS IN UMTS

Na slikah 3 in 4 so prikazani protokolni skladi elementov, ki v omrežjih GPRS in UMTS sodelujejo pri prenosu paketov med mobilnim terminalom in zunanjim paketnim omrežjem, npr. internetom.



slika 3: protokolni skladi v GPRS



slika 4: protokolni skladi v UMTS

Kot vidimo, se aplikacijski podatki in podatki aplikaciji pripadajočega protokola omrežnega sloja prenašajo transparentno med mobilno postajo in prehodnim podpornim vozliščem GPRS (GGSN). Dostopovni del omrežja GPRS ali UMTS z elementi BSS (Base Station Subsystem), UTRAN (UMTS Terrestial Radio Access Network) in SGSN ne vpliva na te podatke.

2. 3. OPIS DELOVANJA SISTEMA GPRS/UMTS

Vmesnik Gb (Iu) zagotavlja povezavo med dostopovnim delom omrežja in vozliščem SGSN in je v omrežju GPRS običajno izveden s tehnologijo Frame Relay, v omrežju UMTS pa z ATM (Asinhronous Transfer Mode).

Vmesnik Gn predstavlja interno paketno hrbtenico v sklopu omrežja GPRS ali UMTS, zato temu delu omrežja rečemo tudi jedrni del omrežja GPRS (GPRS core, UMTS core). Temelji na protokolu IP in je izveden kot LAN (Local Area Network) ali WAN (Wide Area Network) omrežje. Glavni namen tega omrežja je zagotavljati navidezne povezave med SGSN in GGSN posameznim uporabnikom. Navidezne povezave omogoča protokol GTP (GPRS Tunneling Protocol), ki tvori tunele znotraj katerih se prenašajo podatki, ki jih generira mobilni terminal. Ti podatki so odvisni od točke APN kamor se uporabnik priključuje in so lahko IP paketi, PPP paketi ali paketi katerega drugega protokola.

Preko vmesnika Gi prehaja komunikacija v javno podatkovno omrežje. Tu je z dostopovno točko (AP) določeno v katero omrežje se bodo usmerjali paketi, lahko gre npr. za neposredni dostop v javni internet ali za tunel, ki vodi v nek intranet. Za uporabo teh storitev ima vsak uporabnik v bazah podatkov omrežja (HLR, Home Location Register) zapisane podatke o omrežjih kamor se lahko priključi, podatek o omrežnem naslovu, ki ga lahko dodeli tudi strežnik DHCP (Dynamic Host Configuration Protocol) mobilnega operaterja, parameter QoS (Quality Of Service) in še nekatere podatke povezane z administriranjem.

V zvezi z APN velja omeniti še t. i. APN usmerjanje, ki je neke vrste ekvivalent IP usmerjanju, le da APN usmerjanje ne gleda naslovov IP paketov pač pa usmerja glede na pripadnost APN. Metoda se uporablja za direktno usmerjanje paketov iz tunela GTP v tunel v zunanjem paketnem omrežju. Pri tem usmerjevalnik oz. prehod (GGSN) ne obdeluje posameznih paketov, kar je posebnega pomena zlasti pri navideznih zasebnih omrežjih.

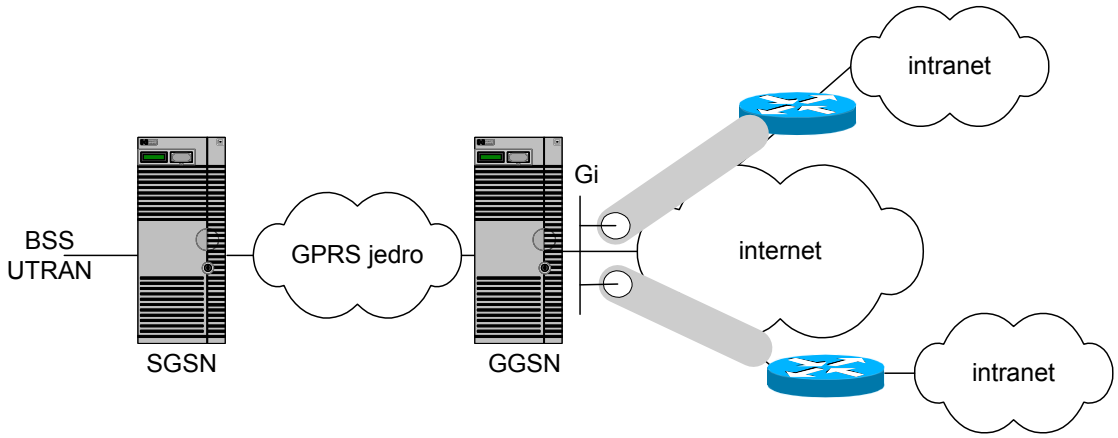
Denimo, da se GGSN povezuje z več intraneti, ki uporabljajo enak naslovni prostor (npr. 10.0.0.0/8). To pomeni, da imamo lahko v omrežju istočasno več mobilnih terminalov z enakim naslovom IP. Ker se paketi skozi lokalno hrbtenico (LAN/WAN) tunelirajo, se srečajo šele na izhodu GGSN, kjer bi lahko prišlo do zmede zaradi enakih IP naslovov. Pri uporabi usmerjanja APN in tuneliranja skozi internet se to, kot smo že opisali, ne zgodi.

2. 4. POVEZOVANJE S PAKETNIMI OMREŽJI IP

Jedrni del omrežja GPRS je povsem ločen od javnega paketnega omrežja oz. interneta, kar omogoča uporabo zasebnih naslovov. Ta del omrežja niti nima neposrednga vpliva na podatkovne pakete z uporabniškimi podatki.

Kot je bilo že omenjeno, za povezavo v omrežje in dodeljevanje naslovov skrbi vozlišče GGSN. V zvezi z dodeljevanjem naslovov ločimo nekaj različnih primerov:

- uporabnikom, ki se povezujejo v intranet svojega podjetja, se naslove dodeljuje v skladu z naslovno shemo intraneta;
- uporabnikom, ki dostopajo v internet se dodelijo zasebni naslovi, njihovi paketi pa v internet prehajajo preko strežnika NAT;
- možna je tudi uporaba javnih naslovov, kar hkrati pomeni, da je uporabnik dosegljiv tudi za t. i. »push« storitve (primer push storitve je poštni strežnik, ki obvešča mobilni terminal o novi pošti, za kar pa potrebuje njegov nedvoumen naslov).



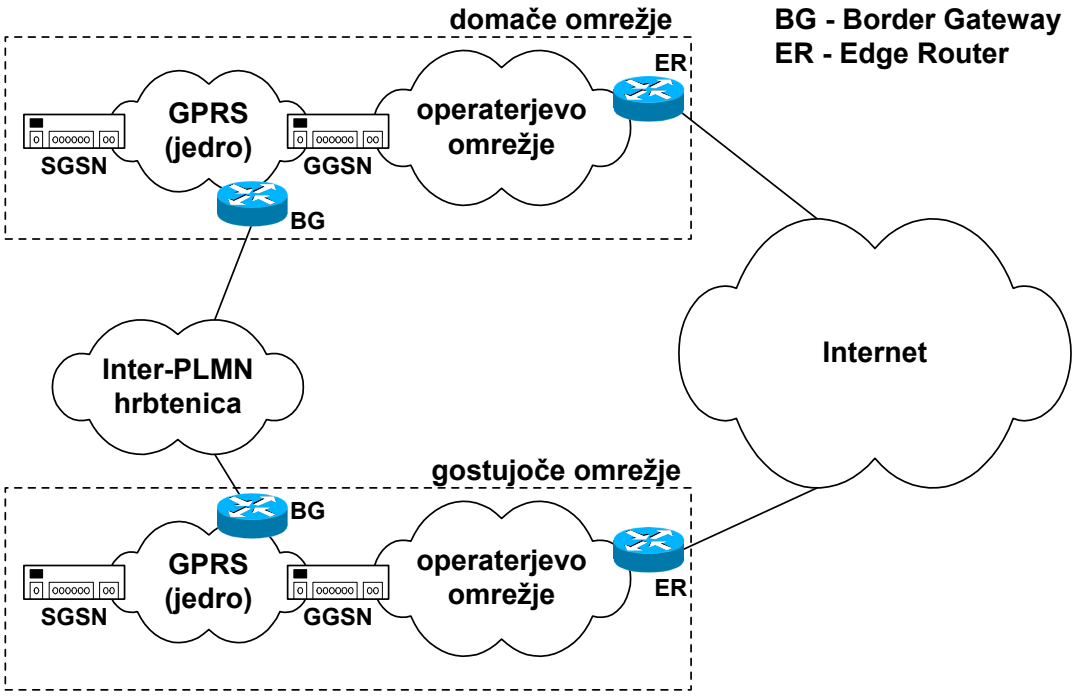
slika 5: povezovanje omrežja GPRS z javnimi omrežji

Dolgoročno je v internetu zagotovo edina rešitev uvedba protokola IPv6, ki ima zadosti velik naslovni prostor, da bi vse naprave lahko uporabljale javne naslove. V razmerah IPv4 je uporaba preslikave naslovov NAT sicer uporabna rešitev, vendar ne najbolj učinkovita. Težave so s t. i. »push« storitvami, ko strežnik pošlje zahtevo mobilnemu terminalu. Kljub rešitvam v obliki strežnikov »Push Proxy Gateway« bo verjetno končna rešitev IPv6.

2. 5. GOSTOVANJE V OMREŽJIH GPRS

Gostovanje GPRS mobilnega uporabnika v omrežju drugega operaterja je možno na dva načina:

- dostop v javno paketno omrežje (internet) preko domačega GGSN;
- dostop v javno paketno omrežje (internet) preko GGSN omrežja v katerem se uporabnik nahaja.



slika 6: inter-PLMN hrbtenično omrežje

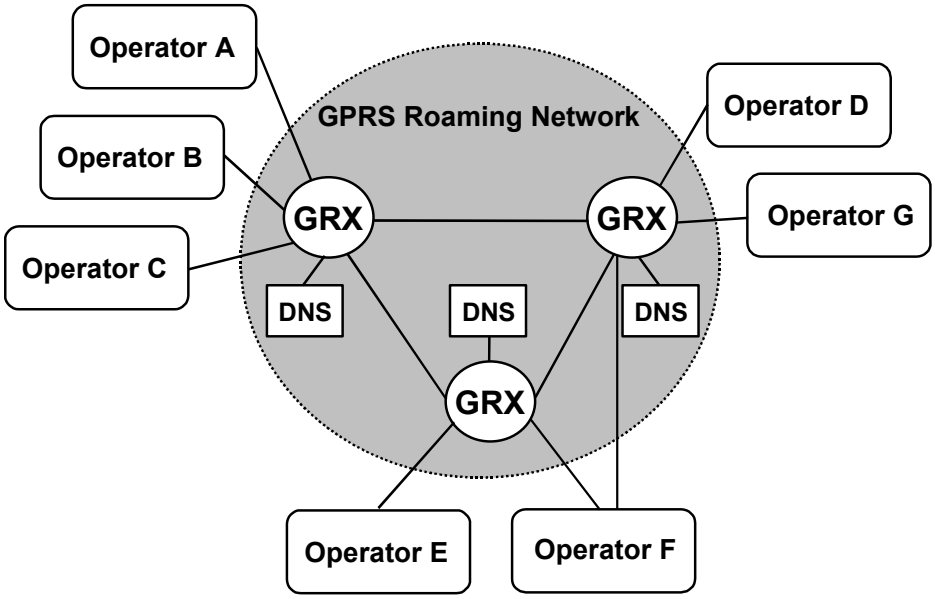
Kadar se GPRS mobilni uporabnik nahaja v tujem omrežju in za prehod v internet uporablja domači GGSN je potrebna povezava jedrnih GPRS omrežij različnih operaterjev (jedrnemu delu GPRS omrežja rečemo tudi intra-PLMN, PLMN – Public Land Mobile Network). Omrežje, ki povezuje PLMN omrežja različnih operaterjev se imenuje inter-PLMN hrbtenično omrežje in je nazorneje prikazano na sliki 5. Za inter-PLMN je definiran vmesnik Gp, ki zagotavlja prenos podatkov s tunelskim protokolom GTP.

Povezava intra-PLMN omrežij je možna z neposrednimi povezavami, ki so lahko fizične (točka-točka) ali navidezne, ali z omrežjem GPRS Roaming Network, ki je neke vrste globalno omrežje s katerim se povezujejo GPRS operaterji.

Za povezovanje dveh inter-PLMN omrežij je uporaben (javni) internet, ki največkrat predstavlja najbolj enostaven način povezave, poleg tega so znani načini še uporaba omrežij ATM, Frame Relay, PPP povezav in navideznih zasebnih omrežij. V primeru interneta je potrebna zaščita prometa, ki se običajno izvaja s protokolom IPsec. Podatki, ki potujejo preko inter-PLMN omrežja se namesto k GGSN usmerijo na poseben prehod (border gateway), ki povezuje domači jedrni del omrežja z gostujočim omrežjem oz. omrežjem, ki zagotavlja povezavo.

Inter-PLMN hrbtenično omrežje oz. GPRS Roaming Network (trenutno) deluje z omrežnim protokolom IPv4 in uporablja javne naslove. Medomrežno povezovanje se izvaja s tunelskim protokolom GTP. Operaterji priključujejo omrežja na vozlišča GRX (Gprs Roaming eXchange), poleg teh vozlišč pa so pomemben sestavni del tudi strežniki DNS (Domain Name Servers). Povezava GPRS omrežja z vozliščem GRX se izvaja z enakimi postopki kot prej omenjeno povezovanje inter-PLMN omrežij.

S stališča uporabnikovega protokola je povsem vseeno kateri protokol se uporablja v inter-PLMN in intra-PLMN omrežjih, saj se skozi ta omrežja uporabniški paketi tunelirajo.



slika 7: GPRS Roaming Network

3. MOBILNOST V OMREŽJIH IP

Cilj mobilnosti je zagotoviti dostop do poljubnega vozlišča na tak način, da bi ga vsakič naslovili z enakim naslovom, neglede na to kje se vozlišče dejansko nahaja. Dober primer rešitve problema mobilnosti so mobilna omrežja, kjer je mobilni uporabnik, točneje SIM kartica, vedno dosegljiv na enaki telefonski številki.

Glavna ovira za mobilnost v omrežjih IP je, da IP naslovi niso prenosljivi – so krajevno odvisni. Vsako omrežje ima svoj naslovni prostor, ki obsega določeno število naslovov. Vozlišče (naprava, terminal), ki je priključeno v omrežje ima omejeno možnost izbire. Če se vozlišče premakne iz enega omrežja v drugega, mora obvezno zamenjati tudi IP naslov.

Opisana lastnost ni v skladu z zahtevo za mobilnost, zato je potrebno težavo rešiti na drugačen način. Ena izmed možnosti bi bilo naslavljanje vozlišč z imeni. Za preslikovanje imen in naslovov se uporablja domenski strežnik (DNS, Domain Name Server), ki bi v takem primeru moral vsebovati zelo obsežno bazo imen in naslovov. Ažurnost podatkov je tu ključnega pomena, vendar pa so DNS strežniki optimirani na iskanje in ne na osveževanje podatkov. Realizacija in vzdrževanje takega strežnika bi bilo precej zapleteno opravilo.

3. 1. PROTOKOL "MOBILE IP"

Rešitev problema mobilnosti je protokol Mobile IP, ki omogoča mobilnost kljub vsem opisanim oviram v omrežjih IP. Protokol Mobile IP je definiran za obe aktualni verziji protokola IP – IPv4 in IPv6. Mobile IPv6 pravzaprav niti še ni dokončno definiran, saj zaenkrat obstaja zgolj standardizacijsko priporočilo IETF v obliki draft (v času pisanja te seminarske naloge je bila aktualna izdaja z dne 1. junij 2002).

Za Mobile IPv4 obstaja nekaj praktičnih realizacij, ki pa so bolj ali manj le eksperimentalnega značaja. Omenimo nekaj organizacij, ki so razvile konkretne izvedbe. Vse delujejo z operacijskim sistemom Linux:

- HP Labs Bristol,
- University of Singapore,
- University of Binghampton,
- Portland State University itd.

Realizacija mobilnosti za IPv6 je morda enostavnejša kot za IPv4, ker Mobile IPv6 lahko s pridom izkoristi opcijske glave protokola IPv6, ki jih v IPv4 ni. Med poskusnimi implementatorji omenimo navezo Microsoft in University of Lancaster. Ker se protokol mobilnosti za IPv4 ni posebej razširil, lahko pričakujemo njegovo splošno uporabo kvečjemu v omrežjih IPv6. Zaradi tega se bo nadaljna obravnava protokola Mobile IP nanašala na zagotavljanje mobilnosti v omrežjih IPv6 (Mobile IPv6).

3. 2. OPIS DELOVANJA PROTOKOLA "MOBILE IPv6"

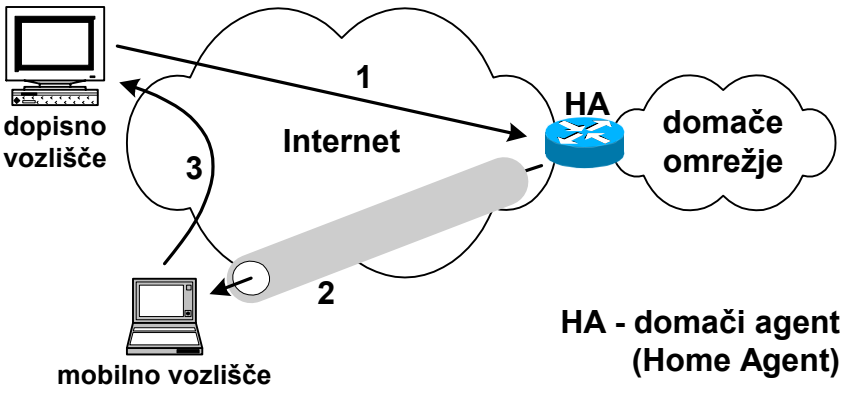
Glavna novost, ki jo uvaja protokol Mobile IP, je domači agent, ki rešuje težave zaradi neprenosljivosti naslovov IP. To je vozlišče, ki po potrebi sodeluje v komunikaciji med

mobilnim vozliščem in vozliščem, ki želi z njim komunicirati. Slednjemu rečemo tudi dopisno vozlišče (correspondent node).

Protokol Mobile IP opravlja štiri pomembne naloge:

- iskanje domačega agenta (Agent Discovery): vsako mobilno vozlišče mora biti registrirano pri svojem domačem agentu, če želi uporabljati storitve mobilnosti;
- registracija (Registration): ko se mobilno vozlišče priključi v tuje omrežje, obvesti svojega domačega agenta o novi lokaciji oz. naslovu IP;
- tuneliranje (Tunneling): kadar se mobilno vozlišče nahaja izven domačega omrežja domači agent prestreza pakete, ki so naslovljeni na domači naslov mobilne naprav in jih tunelira do prejemnika;
- optimizacija usmerjanja (Route Optimization): če dopisnemu vozlišču posredujemo začasni naslov mobilnega vozlišča se izognemo tuneliranju.

Ponazorimo pomen glavnih funkcij protokola Mobile IP z opisom enostavnega primera (slika 8).



slika 8: delovanje protokola

- Mobilno vozlišče se priključi v omrežje, ki ni njegovo domače omrežje.
- Na podlagi sporočil, ki jih razpošilja glavni usmerjevalnik omrežja kamor je priključeno mobilno vozlišče, ugotovi, da se nahaja v tujem omrežju. Mobilno vozlišče pridobi nov, začasen IP naslov (care-of address). IPv6 pozna več načinov dodeljevanja naslovov, lahko so naslovi za gostujoča vozlišča določeni vnaprej.
- Mobilno vozlišče o novem naslovu obvesti svojega domačega agenta – opravi registracijo.
- Domači agent prestreže vse pakete (oznaka 1 na sliki 7), ki so naslovljeni na domači naslov mobilnega vozlišča in jih nato pošlje (tunelira) naslovljenemu vozlišču (2).
- Nadaljnja komunikacija med napravam lahko poteka brez sodelovanja domačega agenta (3).
- Tuneliranju se izognemo, če dopisno vozlišče obvestimo o začasnem naslovu mobilnega vozlišča – mu posredujemo vezi (optimizacija usmerjanja).

Vez (Binding) je podatek o trenutnem naslovu mobilnega vozlišča, kadar to gostuje – se ne nahaja v domačem omrežju.

Najbolj kompleksna naprava protokola Mobile IPv6 je domači agent, saj izvaja obsežen nabor funkcij. V dosedaj poznanih izvedbah protokola Mobile IPv6 so načrtovalci imeli največ težav prav z nestabilnim delovanjem domačega agenta.

Glavna naloga domačega agenta je vzdrževanje baze o aktualnih vezeh mobilnih vozlišč. Glavna podatka baze sta domači in začasni naslov mobilnega vozlišča. Mobilno vozlišče sporoči potrebne podatke ob registraciji, ko od domačega agenta zahteva izvajanje storitev mobilnosti. Storitev mobilnosti je predvsem prestrezanje paketov, ki so naslovljeni na domači naslov in tuneliranje teh paketov na nov naslov mobilnega vozlišča. Poleg registracije je potreben še postopek deregistracije, ko se mobilno vozlišče odjavi pri domačem agentu, ki od tedaj dalje zanj ne opravlja več storitev mobilnosti.

Pri poskusu registracije lahko pride do težav, če je v času, ko mobilnega vozlišča ni bilo v domačem omrežju, prišlo npr. do zamenjave domačega agenta, ki morda niti nima več enakega IP naslova. V takem primeru domači agent ne pozna mobilnega vozlišča in zavrne njegovo zahtevo za registracijo. V nekem omrežju je lahko aktivnih več domačih agentov in če je bil eden od agentov zamenjan ali kako drugače umaknjen iz omrežja, njegove stranke (mobilna vozlišča) prevzame drug domači agent. Mobilno vozlišče, ki je bilo zdoma mora torej ugotoviti pri katerem domačem agentu se lahko registrira. V ta namen IPv6 uporablja postopek dinamičnega iskanja domačega agenta (Dynamic Home Agent Discovery), ki deluje po naslednjem principu:

- mobilno vozlišče pošlje zahtevo za registracijo,
- paket prestreže eden izmed domačih agentov v domačem omrežju mobilnega vozlišča,
- domači agent poroča mobilnemu vozlišču o neuspešnosti registracije in zraven doda spisek vseh delujočih agentov domačega omrežja,
- mobilno vozlišče se registrira pri ustreznem agentu.

Med možnimi vzroki neuspešnosti registracije najdemo tudi:

- pomanjkanje virov domačega agenta: domači agent je zaseden in ni možno, da bi se ukvarjal s še enim mobilnim vozliščem, tak primer bi moral biti redkost,
- neuspela avtentikacija ali identifikacija: pri postopku registracije je posebnega pomena varnost, saj ne želimo nepooblaščenih registracij,
- neustrezno definirana zahteva za registracijo,
- napačno naslovljen domači agent: probleme, ki se rešuje s postopkom dinamičnega iskanja domačega agenta.

Za registracijo se uporablja dvoje različnih protokolnih sporočil:

- Binding Update: poskus oz. zahteva za registracijo,
- Binding Acknowledgment: sporočilo o uspešnosti registracije.

Zgradba protokolnih sporočil je podrobneje predstavljena v poglavju o glavi mobilnosti (Mobility Header), tu pa omenimo, da med pomembnejšimi podatki, ki jih mobilno vozlišče posreduje ob registraciji najdemo še predviden čas uporabe začasnega naslova. Domači agent v povratnem sporočilu mobilnemu vozlišču predvideni čas uporabe potrdi ali pa ga (samostojno) skrajša, nikoli pa ga ne podaljša.

3. 3. GLAVA MOBILNOSTI

Glava mobilnosti (Mobility Header) nastopa v IPv6 paketu kot opcija. To glavo uporabljajo mobilna vozlišča, dopisna vozlišča in domači agenti v vseh sporočilih, ki se nanašajo na vzpostavljanje in vzdrževanje vezi.

Zgradbo glave mobilnosti prikazuje slika 9. Glava, ki v paketu IPv6 nastopa pred glavo mobilnosti slednjo napove v polju naslednja glava (Next Header).

slika 9: glava mobilnosti (Mobility Header)

- **Naslednji protokol**: 8-bitna vrednost označuje glavo, ki sledi glavi mobilnosti. Uporaba tega polja je predvidena v prihodnosti in je povezana z varnostnimi mehanizmi, v trenutnem stanju pa se v to polje vpiše vrednost NO_NXTHDR (ni naslednje glave).

- **Dolžina glave**: dolžina celotne glave mobilnosti, vključno z vrednostjo »naslednji protokol«. Osnovna enota za podajanje dolžine glave je 8 oktetov, iz česar sledi, da je dolžina glave mobilnosti vedno večkratnik 8 oktetov.

- **MH**: oznaka vrste sporočila, ki se prenaša (Binding Refresh Request, Binding Update, Binding Acknowledgement, Home Test Init, Care-of Test Init ipd.).

- **Kontrolna vsota**: kontrolna vsota (checksum) glave mobilnosti.

- **Podatki**: podatki, ki jih določa oznaka vrste sporočila (MH).

Poleg standardnih sporočil so predvidene tudi opcije mobilnosti – mobility options. Opcije so pripete za podatki prenašanega sporočila, njihov obstoj pa se ugotavlja na podlagi dolžine paketa. Dolžine standardnih sporočil so predpisane in zato vnaprej znane. Če je vrednost v polju dolžina glave večja od pričakovane, to pomeni, da so v paket vključene tudi opcije mobilnosti. Pri tem velja še enkrat opozoriti na dejstvo, da mora biti tudi dolžina opcij deljiva z 8 okteti, za izpolnitev te zahteve pa je občasno potrebno dodajati polnilne bite.

Poleg že znanih sporočil za upravljanje z vezmi, Mobile IP pozna še sporočila za zagotavljanje varnosti s pomočjo avtentikacije in identifikacije vozlišč. Več o varnosti je napisano v poglavju 3.5. V nadaljevanju naštejmo vsa standardna sporočila, ki jih v glavi mobilnosti najdemo v podatkovnem polju:

- zahteva za osveževanje vezi (Binding Refresh Request): poskus oz. zahteva za osveževanje vezi, dopisno vozlišče pri mobilnem vozlišču zahteva sveže podatke o vezeh;
- osvežitev vezi (Binding Update): mobilno vozlišče s tem sporočilom ostalim (zainteresiranim) vozliščem sporoči o svojem novem začasnem naslovu;
- potrditev osvežitve vezi (Binding Acknowledgment): s tem sporočilom vozlišče odgovori, da je prejelo podatke o novih vezeh (osvežitev vezi), v sporočilu je navedeno ali je osvežitev vezi uspela ali ne;
- napaka (Binding Error): to sporočilo uporabi dopisno vozlišče, če ugotovi težave povezane z vezmi;

- začetek domačega preizkusa (Home Test Init Message): mobilno vozlišče pošlje dopisnemu vozlišču sporočilo, ki vsebuje domači piškotek (Home Test Cookie – HoT) in od njega zahteva, da mu ta piškotek vrne s čimer preverja njegovo avtentičnost;
- začetek začasnega preizkusa (Care-of Test Init Message): podobno kot pri domačem preizkusu, le da gre tu za drug piškotek (Care-of Test Cookie – CoT);
- domači preizkus (Home Test Message): odziv dopisnega vozlišča na prejeto zahtevo za domači preizkus, dopisno vozlišče vključi še svoj domači piškotek da lahko kontrolira mobilno vozlišče;
- začasni preizkus (Care-of Test Message): odziv dopisnega vozlišča na prejeto zahtevo za začasni preizkus, podobno kot pri domačem preizkusu tudi pri začasnem preizkusu dopisno vozlišče vključi svoj začasni piškotek.

Omenili smo tudi opcije mobilnosti, ki se po potrebi dodajajo glavi mobilnosti. Hkrati se lahko doda ena ali več opcij, ti podatki pa so prav tako kot standardna sporočila vključeni v podatkovno polje glave mobilnosti.

vrsta opcije	dolžina opcije	opcijski podatki

slika 10: opcije

Trenutno (Mobility Support in IPv6, IETF draft version 18) so specificirane naslednje opcije:
- polnilo 1: polnilni biti dolžine 1 oktet;
- polnilo N: polnilni biti dolžine N oktetov, ki se dodajajo kadar je potreba po polnilnih bitih dolžine več kot 1 oktet;
- identifikator neponovljivosti (Unique Identifier);
- alternativni začasni naslov (Alternate Care-of Address);
- indeks naključno generiranih vrednosti (Nonce Indices): vsako vozlišče generira več naključnih vrednosti, ki se uporabljajo za identifikacijo, med vozliščema pa se prenašajo samo kazalci, ki povejo katera naključna vrednost je v danem primeru aktualna;
- avtorizacija vezi (Binding Authorization Data): na podlagi šifriranih podatkov te opcije se je možno natančno prepričati o izvornosti vezi;
- nasvet za osveževanje vezi (Binding Refresh Advice): domači agent pripne to opcijo k sporočilu o potrditvi registracije, s to opcijo domači agent priporoča mobilnemu vozlišču časovni interval osveževanja podatkov.

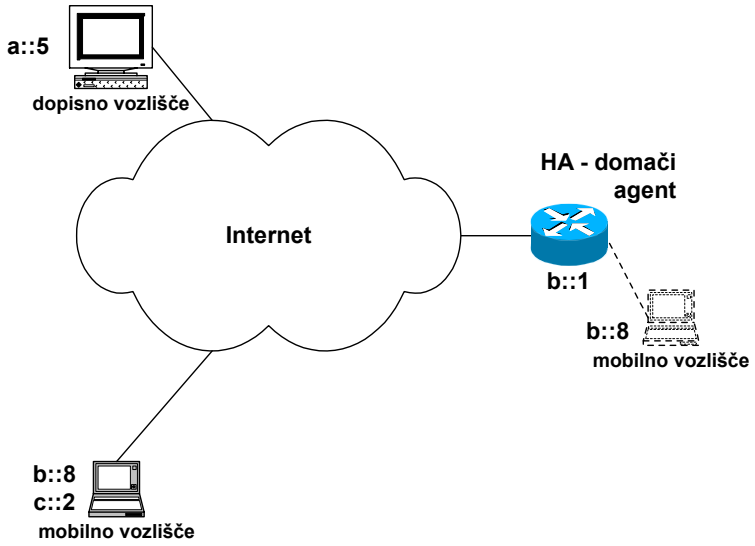
3. 4. OPTIMIZACIJA USMERJANJA

Cilj optimizacije usmerjanja je izločitev domačega agenta pri neposredni komunikaciji mobilno vozlišče – dopisno vozlišče. Domači agent se uporabi le ob vzpostavitvi povezave, v nadaljevanju pa je pošiljanje paketov s posredovanjem domačega agenta običajno dokaj neoptimalno.

Postopek je videti zelo preprost – dopisnemu vozlišču pošljemo podatke o začasnem naslovu mobilnega vozlišča (osvežimo njegovo bazo vezi) in vozlišči od tedaj naprej lahko komunicirata brez posredovanja domačega agenta. Izvedba napisanega pa ni tako enostavna, prvi problem je že zagotavljanje ažurnosti podatkov v bazi vezi dopisnega vozlišča. Reševanje tega problema smo do neke mere že obdelali v predhodnih poglavjih.

Zamislimo si primer omrežja IPv6, ki ga prikazuje slika 11. Mobilno vozlišče ima v domačem omrežju naslov b::8, trenutno pa gostuje in ima začasen naslov c::2. Dopisno vozlišče ima naslov a::5, domači agent mobilnega vozlišča pa b::1.

Ponorni naslov v glavi prvega paketa, ki ga dopisno vozlišče pošlje mobilnemu vozlišču, je domači naslov mobilnega vozlišča. Na transportnem nivoju (protokol TCP) se vzpostavi seja, ki je določena z obema IP naslovoma (izvorni in ponorni naslov) in oznako vrat, npr. 80 za HTTP dostop.



slika 11: primer omrežja z mobilnim vozliščem

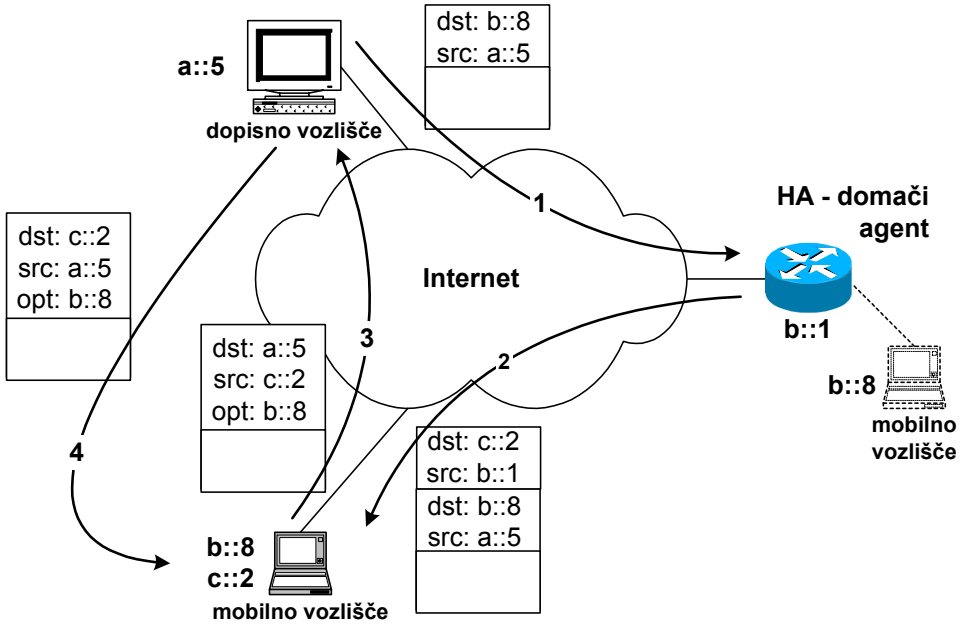
Ko paket prispe do domačega omrežja mobilnega vozlišča, ga prestreže domači agent, ki ve da je mobilno vozlišče zdoma, zato mu paket tunelira. Izvorni naslov tunela je naslov domačega agenta, ponorni pa začasni naslov mobilnega vozlišča. Poznamo več tunelskih protokolov, za uporabo v Mobile IP se predvidevajo predvsem: GRE (Generic Routing Encapsulation), Minimal Encapsulation in IP-within-IP encapsulation.

Mobilno vozlišče sprejme paket in tedaj lahko steče osveževanje baze vezi dopisnega vozlišča. Odgovor na prejeto zahtevo (podatki v paketu, ki jih je poslalo dopisno vozlišče) mobilno vozlišče lahko pošlje neposredno dopisnemu vozlišču. Pomembno pri tem je, da mobilno vozlišče v IP paketu kot izvor navede svoj domači naslov, saj bi sicer prišlo do prekinitve zveze na nivoju TCP seje. Takšno »pretvarjanje« načeloma ni problematično, saj je podatek o izvoru v fazi usmerjanja nepomemben. Zaplete se, ko mobilno vozlišče gostuje v omrežju zaščitenem s požarnim zidom. Filtri v požarnih zidovih običajno kontrolirajo tudi izvorne naslove in v primeru, ko izvorni naslov ni ustrezen (ne pripada podomrežju) paket zavrnejo. Problem je rešen z uporabo ponorne opcije (Destination Option), ki jo predvideva osnovna izvedba protokola IPv6. V glavi IP paketa je kot izvor naveden začasen naslov mobilnega vozlišča, njegov domači naslov pa je dodan kot opcija, kar je dovolj, da dopisno vozlišče ne prekine seje.

Težava z naslovi se nato pojavi, ko želi dopisno vozlišče neposredno poslati paket mobilnemu vozlišču, saj ga mora nasloviti z njegovim začasnih naslovom kar je zopet v nasprotju z zahtevo TCP seje. Dopisno vozlišče uporabi opcijo usmerjanja (Routing Option), ki je prav tako del osnovne izvedbe IPv6. V resnici se za Mobile IP uporablja nekoliko spremenjena izvedba opcije usmerjanja, ki je modificirana tako, da lahko vsebuje le en IPv6 naslov. V

glavi IP paketa je kot ponor naveden začasen naslov mobilnega vozlišča, njegov domači naslov pa je dodan kot opcija.

V nadaljevanju poteka komunikacija med mobilnim in dopisnim vozliščem z uporabo opcij po pravkar opisanem scenariju. Boljši pregled nad situacijo nam daje slika 12, ki povzema opisani postopek. Slika se osredotoča zgolj na optimizacijo usmerjanja paketov z aplikacijskimi podatki in ne vsebuje postopkov osveževanja vezi. Poseben poudarek je dan glavam paketov – na sliki vidimo najpomembnejše podatke v glavi: izvorni in ponorni naslov ter opcije. Paket pod puščico »2« je tunelirani paket – prvo (zgornje) polje predstavlja zunanjo glavo, drugo (srednje) polje pa notranjo glavo.



slika 12: potek komunikacije v Mobile IPv6

3. 5. VARNOST PRI UPORABI PROTOKOLA MOBILE IP

Tudi pri uporabi protokola Mobile IP se srečamo z vprašanjem varnosti. Varnost je potrebno zagotoviti pri registraciji in osveževanju vezi, saj ne želimo, da bi npr. kdo zlorabljal našega domačega agenta ali da pri osveževanju vezi ne bi vedeli komu pravzaprav zaupamo.

Varnost je v protokolu Mobile IP zagotovljena z identifikacijo in avtentikacijo. Načina izvedbe pa sta dva:

- na relaciji mobilno vozlišče – domači agent se uporablja protokol IPsec;
- med mobilnim vozliščem in dopisnim vozliščem pa se identifikacija in avtentikacija izvaja s piškotki (Cookies).

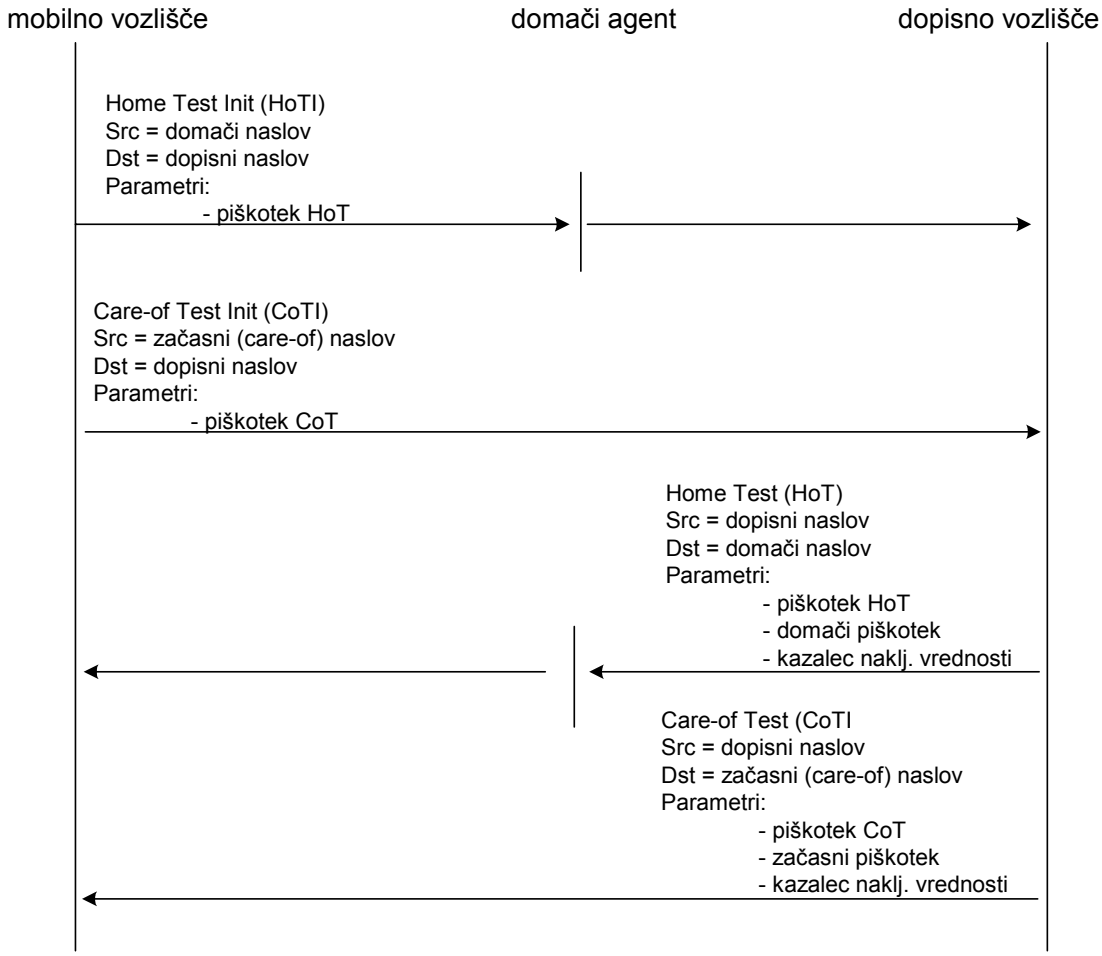
Protokol IPsec (Internet protocol Security) je obvezni sestavni del protokola IPv6, omogoča pa kontrolo dostopa, avtentikacijo podatkov in izvora podatkov, šifriranje podatkov, zaščito pred podvajanjem paketov, nepovezavno celovitost in delno zaupnost prometnega pretoka.

Zaščita podatkov z uporabo piškotkov je nekoliko bolj zapletena in temelji na izmenjavi piškotkov med mobilnim in dopisnim vozliščem. Postopek izmenjave teh sredstev se imenuje Return Routability Procedure.

Kot je bilo omenjeno v poglavju 3.3 se poleg različnih vrst piškotkov uporabljajo še naključne vrednosti (Nonce), ki se ne prenašajo v izvorni obliki pač pa ima vsaka vrednost svoj kazalec dolžine 16 bitov.

Razlikujemo piškotke treh vrst:
- domači piškotki, ki jih generira mobilno vozlišče in jih pošlje dopisnemu vozlišču, to sta piškotka HoT in CoT;
- domači piškotek (home cookie), ki ga generira dopisno vozlišče in ga preko domačega agenta pošlje mobilnemu vozlišču;
- začasni piškotek (care-of cookie), ki je podoben domačemu vendar ga dopisno vozlišče pošlje neposredno mobilnemu vozlišču.

Postopek izmenjave je prikazan na sliki 12, sporočila, ki se uporabljajo smo podrobneje opisali v poglavju 3.3.



slika 13: Return Routability Procedure

Ko mobilno vozlišče sprejme nazaj piškotka HoT in CoT je proces preverjanja končan. Mobilno vozlišče je oskrbljeno s potrebnimi podatki za dokazovanje avtoritete in lahko začne s pošiljanjem podatkov za osvežitev vezi.

4. PREHOD IZ IPv4 V IPv6 V OMREŽJIH GPRS IN UMTS

Zgradbo in delovanje omrežij GPRS in UMTS smo podrobno opisali v poglavju 2, tu pa nas bo zanimala predvsem uporaba oz. vpeljava protokola IPv6 v ta omrežja. V mobilnih paketnih omrežjih se protokoli paketnega prenosa podatkov pojavljalo na dveh ločenih nivojih (jedrni del omrežja in uporabniški podatki), zato tudi pri uvajanju IPv6 lahko govorimo o dveh različnih tematikah, ki med sabo nista odvisni.

Pri uvajanju protokola IPv6 v mobilna paketna omrežja gre tako v primeru jedrnega dela omrežja kot pri problemu uporabniških podatkov za enake prijeme in postopke. Razlika je predvsem v tem, da je v primeru jedrnega dela omrežja in hrbtenice PLMN uvajanje novega protokola odvisno od operaterjev, v primeru uporabniških podatkov pa od želja in zahtev uporabnikov.

Glavna prednost protokola IPv6 za omrežja GPRS in UMTS je obsežen naslovni prostor in s tem možnost, da vsaka naprava v mobilnem omrežju dobi javen IP naslov. Potreba po javnem naslovu je, kot smo opisali v poglavju 2, povezana s storitvami, ki so gibalo razvoja mobilnih omrežij in prav zato je pričakovati prve izvedbe IPv6 na uporabniškem nivoju. V nadaljevanju se bomo pretežno posvetili pričakovanemu dogajanju v mobilnih omrežjih, ko se bodo začeli pojavljati terminali z IPv6 protokolnimi skladi.

Za podporo mobilnosti je tudi v omrežjih GPRS in UMTS uporaben protokol Mobile IP. Uporaben je pri gostovanju v omrežjih GPRS in UMTS drugih mobilnih operaterjev kot tudi v mikro in piko celicah, ki se bodo pojavile z razvojem omrežij naslednje generacije. Te celice bodo delovale z različnimi tehnologijami, npr. WLAN (Wireless Local Area Network), Bluetooth, DECT ipd. Pri preklopu med celicami različnih tehnologij lahko pride do zamenjave IP naslova, to nevšečnost pa se da odpraviti s protokolom Mobile IP. Gostovanje v omrežjih GPRS in UMTS smo podrobneje opisali v poglavju 2. V primeru, ko gostujoči mobilni terminal dostopa v Internet preko prehoda operaterja pri katerem gostuje, je lahko dostopen na domačem naslovu z uporabo protokola Mobile IP.

Uporabo IPv6 v omrežjih GPRS in UMTS predpisujejo tudi standardizacijski dokumenti različnih standardizacijskih teles, omenimo npr. 3GPP (3rd Generation Partnership Project) in IETF (Internet Engineering Task Force).

4. 1. SOOBSTOJ IPv4 IN IPv6

Internet zaenkrat temelji na protokolu IPv4, omrežja IPv6 dosegajo kvečjemu velikosti lokalnih omrežij. Poleg lokalnih IPv6 omrežij poznamo tudi svetovno omrežje oz. hrbtenico IPv6 imenovano 6bone, ki je še v začetni fazi razvoja. V omrežju 6bone najdemo HTTP, FTP, IRC strežnike, ki za komunikacijo na omrežnem sloju uporabljajo IPv6.

Preden bo IPv6 prevladal v Internetu bo minilo še kar nekaj časa, vsekakor se to ne bo zgodilo »čez noč«. Predviden prehod iz IPv4 v IPv6 lahko opišemo s tremi fazami – od pretežno IPv4 Interneta, preko mešanega omrežja do pretežno IPv6 Interneta.

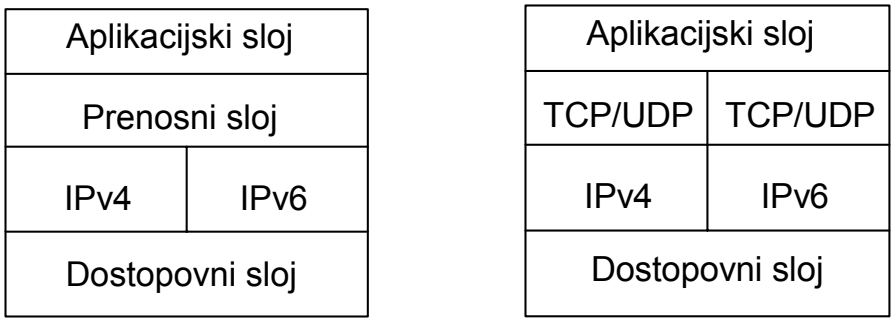
Soobstoj dveh protokolov pri opisani situaciji zahteva postopke za povezovanje ločenih IPv6 omrežij preko omrežja IPv4 ter postopke za povezovanje IPv4 in IPv6 naprav. Ločimo dva osnovna principa:

- dvojni protokolni skladi v napravah in
- tuneliranje.

Ko govorimo o dvojnih protokolnih skladih moramo imeti v mislih, da na tak način uvedemo razlikovanje med napravami. Ločimo:

- izključno IPv4 vozlišče: predstavlja večino današnjih vozlišč, vsebuje le IPv4 protokolni sklad in IPv4 naslov,
- izključno IPv6 vozlišče: nezdružljivo z večino današnjih vozlišč, vsebuje le IPv6 protokolni sklad in IPv6 naslov,
- mešano IPv4/IPv6 vozlišče: implementirana sta oba protokola, prav tako ima vozlišče dva IP naslova, enega IPv4 in enega IPv6,
- IPv4 vozlišče: je lahko izključno IPv4 vozlišče ali mešano vozlišče, pakete pa pošilja in sprejema le po IPv4,
- IPv6 vozlišče: je lahko izključno IPv6 vozlišče ali mešano vozlišče, pakete pa pošilja in sprejema le po IPv6.

Izvedba dvojnega protokolnega sklada obstaja v dveh oblikah. Pri dvojnem IP sloju je ločitev izvedena na omrežnem sloju kjer hkrati tečeta dva protokola, IPv4 in IPv6. Prenosni in aplikacijski sloj poljubno komunicirata s katerimkoli omrežnim protokolom, odvisno od potrebe. Omogočeno je tudi tuneliranje IPv6 paketov v IPv4 zvezi. Protokolni sklad z dvojnim IP slojem je prikazan na levem delu slike 13.



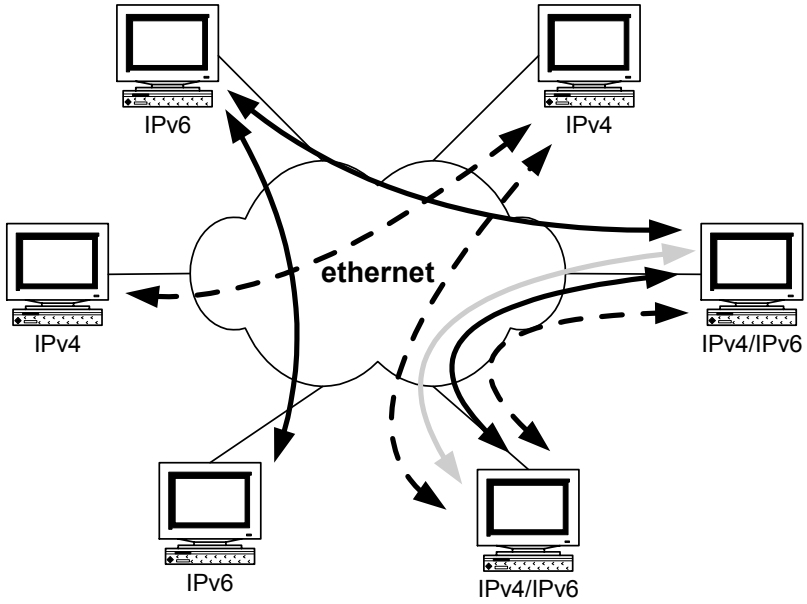
slika 14: dvojni IP sloj (levo) in dvojni TCP/IP protokolni sklad (desno)

V protokolnem skladu z dvojnim TCP/IP skladom je poleg omrežnega protokola ločen tudi protokol prenosnega sloja. Delovanje je podobno kot v primeru dvojnega IP sloja – aplikacija lahko komunicira s poljubnim skladom, omogočeno je tuneliranje. Protokolni sklad z dvojnim TCP/IP skladom prikazuje desna stran slike 13.

Naprava z dvojnim skladom ima hkrati aktivna dva IP naslova (IPv4 in IPv6). Zamislimo si omrežje z dostopovnim protokolom Ethernet, ki vsebuje izključno IPv4, izključno IPv6 in mešana vozlišča (slika 15). IPv6 vozlišče lahko komunicira z IPv6 vozliščem po protokolu IPv6, prav tako lahko z istim protokolom komunicira z mešanim IPv4/IPv6 vozliščem. Z izključno IPv4 vozliščem ne more komunicirati. Podobno lahko izključno IPv4 vozlišče komunicira z drugim IPv4 ali mešanim vozliščem preko protokola IPv4, ne more pa komunicirati z izključno IPv6 vozliščem. Mešani vozlišči pa med sabo lahko komunicirata na tri različne načine:

- s protokolom IPv4,
- s protokolom IPv6 ali
- s tuneliranjem IPv6 paketov preko IPv4.

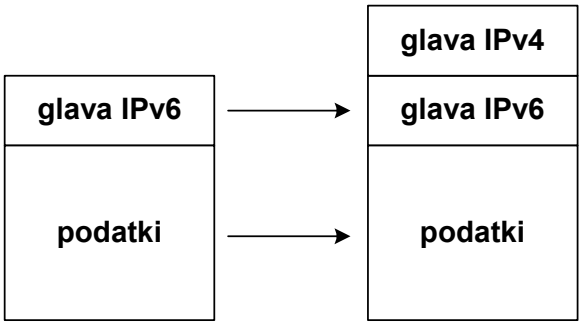
Kot že rečeno, opisano situacijo v mešanem omrežju prikazuje slika 15. Črne povezave na sliki predstavljajo komunikacijo s protokolom IPv6, pikčaste povezave komunikacijo s protokolom IPv4 in siva povezava tuneliranje IPv6 v IPv4.



slika 15: mešano omrežje

Tuneliranje je dobro znana metoda, ki pogosto nastopa v omrežjih IP, omenili smo jo tudi v poglavju o mobilnosti v omrežjih IP. Pri tuneliranju IPv6 paketov preko IPv4 omrežja gre za posredovanje IPv6 paketov med napravami katerih povezava je možno edino po poti, ki vsebuje del IPv4 omrežja. Ker so paketi IPv6 drugačni kot paketi IPv4, jih omrežni elementi IPv4 ne znajo usmerjati, zato uporabimo mešano vozlišče, ki IPv6 paketu doda glavo IPv4. Dodana glava je zadosten pogoj, da paket pravilno potuje po omrežju.

Slika 16 prikazuje osnovni princip tuneliranja paketov IPv6 v paketih IPv4.

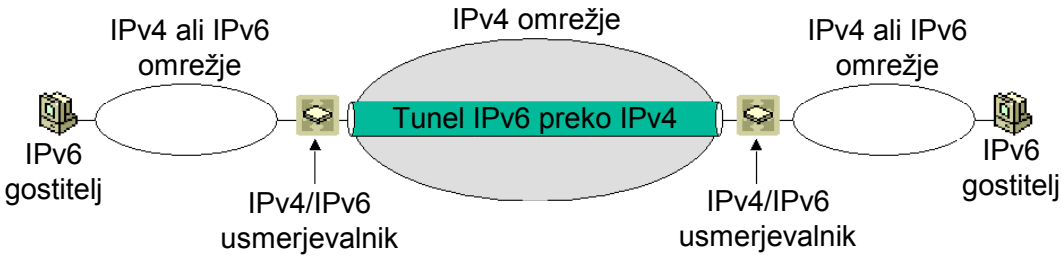


slika 16: tuneliranje

Za nastali tunel lahko rečemo, da je tunel protokola IPv4, saj sta začetna in končna točka tunela naslova IPv4. Konfiguriranje tunela lahko poteka ročno ali samodejno – odvisno od programske izvedbe. Slika 17 na naslednji strani prikazuje tunel med dvema omrežjema kjer je tunel vzpostavlje med usmerjevalnikoma z dvojnim protokolnim skladom.

Poleg tuneliranja med dvema omrežjema oz. tunela usmerjevalnik – usmerjevalnik, lahko tunel vzpostavimo tudi med dvema končnima napravama (tunel gostitelj – gostitelj) ali med omrežjem in končno napravo (usmerjevalnik – gostitelj).

V prihodnosti lahko pričakujemo situacijo, ko bodo prevladovala omrežja IPv6 in bo status omrežij IPv4 pretežno lokalne narave. Takrat se bo pojavila tudi potreba po tuneliranju paketov IPv4 preko omrežij IPv6. Vedno pa bo prisotna potreba po komunikaciji vozlišč, ki delujejo z različnimi protokoli. Izključno IPv4 in izključno IPv6 vozlišče nista kompatibilni, možno pa ju je povezati z vključitvijo protokolnega in naslovnega prevajalnika (NAT-PT, Network Address Translation – Protocol Translation). Funkcija prevajalnika je dobro znana, realizacija pa je možna z dvojnim skladom.



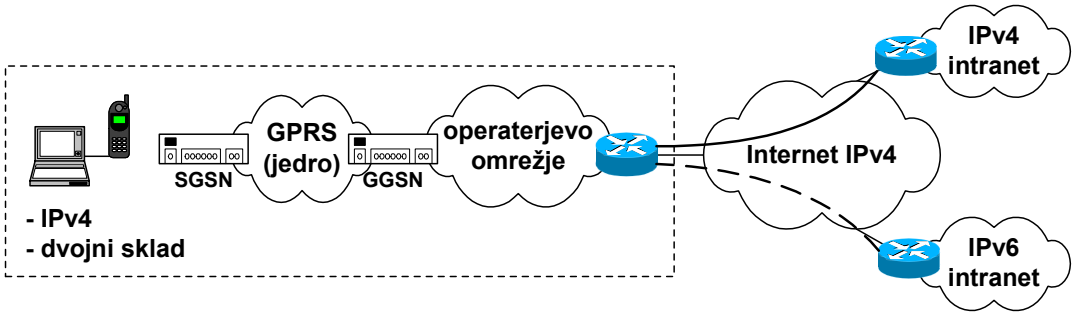
slika 17: tunel usmerjevalnik – usmerjevalnik

Naštejmo nekaj mehanizmov soobstoja IPv4 in IPv6:

- 6over4: tuneliranje paketov IPv6 skozi omrežje IPv4;
- ISATAP (Intra Site Automatic Tunnel Addressing Protocol): tuneliranje paketov IPv6 skozi omrežje IPv4;
- DSTM (Dual Stack Transition Mechanism): tuneliranje paketov IPv4 skozi omrežje IPv6;
- IP-in-IP: tuneliranje IPv6 skozi IPv4 ali tuneliranje IPv4 skozi IPv6;
- NAT-PT (Network Address Translation – Protocol Translation): prevajanje IPv4 v IPv6 in obratno;
- SIIT (Stateless IP/ICMP Translation): prevajanje IPv4 v IPv6 in obratno;
- BIS (Bump-In-Stack): prevajanje IPv4 v IPv6.

4. 2. PREHOD IZ IPv4 V IPv6 V OMREŽJIH GPRS IN UMTS

4.2.1. PRVA FAZA PREHOD

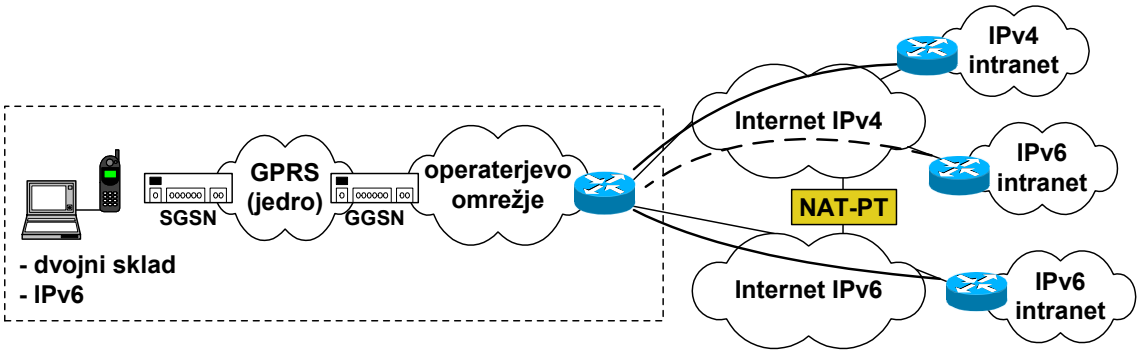


slika 18: prva faza prehoda IPv4 v IPv6

Za prvo fazo prehoda iz IPv4 v IPv6 lahko rečemo, da je to današnje stanje, ko imamo IPv4 Internet, posamezna krajevna IPv6 omrežja in terminale z dvojnim skladom. Mobilni operaterji v tej fazi razvoja večinoma ne ponujajo IPv6 zmogljivosti oz. storitev, zato je

uporaba protokola IPv6 povsem odvisna od uporabnikov. Do storitev temelječih na IPv6 lahko uporabnik dostopa skozi tunel, ki se začne v njegovem terminalu, kar pa ni težava, saj vozlišča z dvojnimi skladi omogočajo gradnjo tunelov.

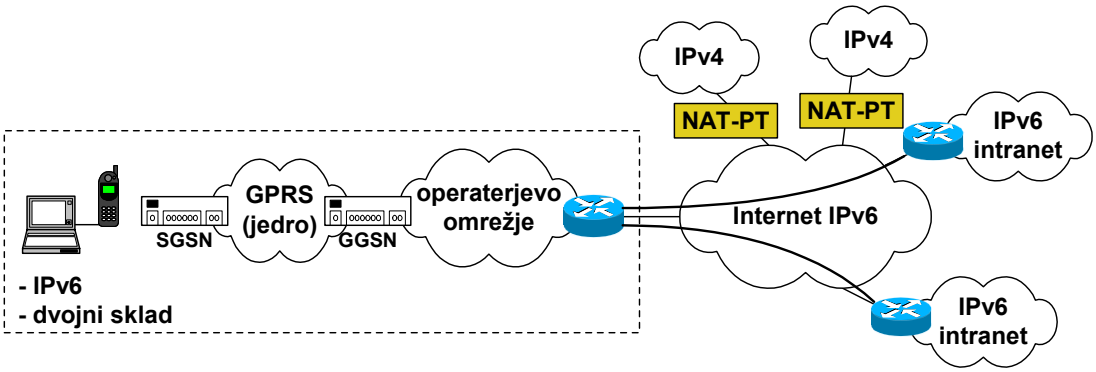
4.2.2. DRUGA FAZA PREHODA



slika 19: druga faza prehoda

O drugi fazi prehoda iz IPv4 v IPv6 bomo govorili, ko bo velikost omrežij IPv6 primerljiva z velikostjo omrežij IPv4. Takrat bodo tudi storitve IPv6 že precej razširjene, pojavili pa se bodo izključno IPv6 terminali. V tej fazi razvoja bo omrežje verjetno najbolj kompleksno, kar bodo občutili predvsem operaterji, ki bodo morali zagotavljati povezljivost z obema protokoloma. Če predpostavimo relativno veliko število izključno IPv4 in IPv6 vozlišč, ugotovimo povečano potrebo po IPv4/IPv6 prevajalnikih. Uporaba tunelov pa se zaradi velike razširjenosti globalnega IPv6 omrežja utegne zmanjšati.

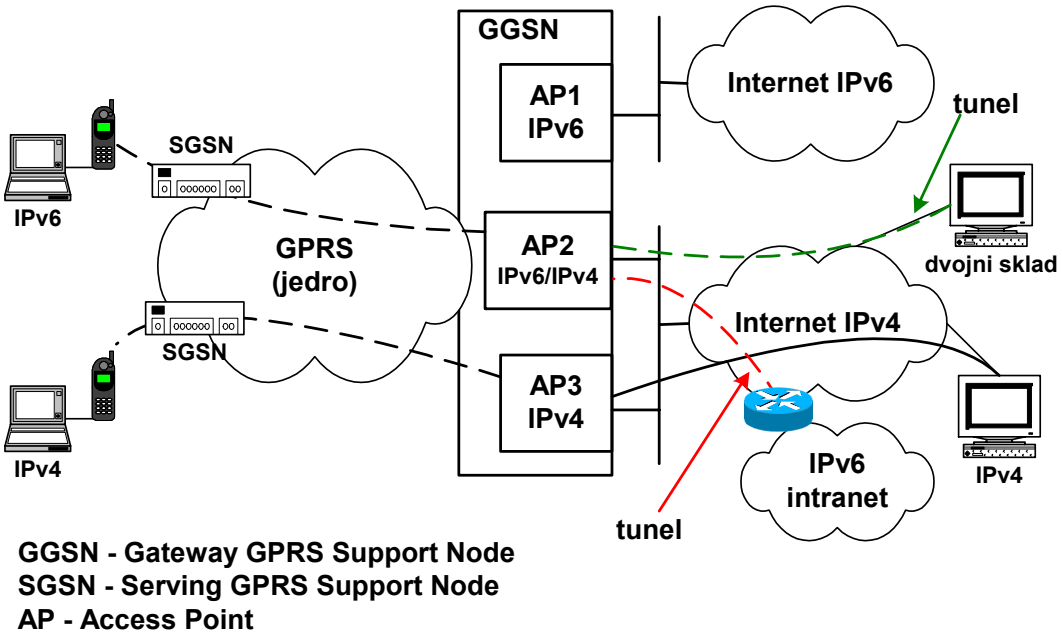
4.2.3. TRETJA FAZA PREHODA



slika 20: tretja faza prehoda

V tretji fazi prehoda bo Internet deloval s protokolom IPv6, prav tako bodo vse storitve dosegljive z IPv6, omrežja IPv4 pa bodo postala obrobnega pomena. Situacija bo obratna situaciji v prvi fazi prehoda IPv4 v IPv6. Pričakujemo lahko, da bodo prav v mobilnih omrežjih terminali IPv4 najhitreje izginili, saj bodo mobilni operaterji uporabnikom bistveno laže zagotovili javni IPv6 kot javni IPv4 naslov.

4.2.4. SOOBSTOJ TERMINALOV IN DOSTOPOVNIH TOČK IPv4 IN IPv6



slika 21: dostopovne točke

Za prehod uporabnikovih podatkov v podatkovno omrežje (Internet) skrbi vozlišče GGSN (Gateway GPRS Support Node – prehodno podporno vozlišče GPRS). Mobilni terminal dostopa v paketno omrežje preko pripadajoče dostopovne točke (AP, Access Point), ki lahko izvaja tudi tuneliranje.

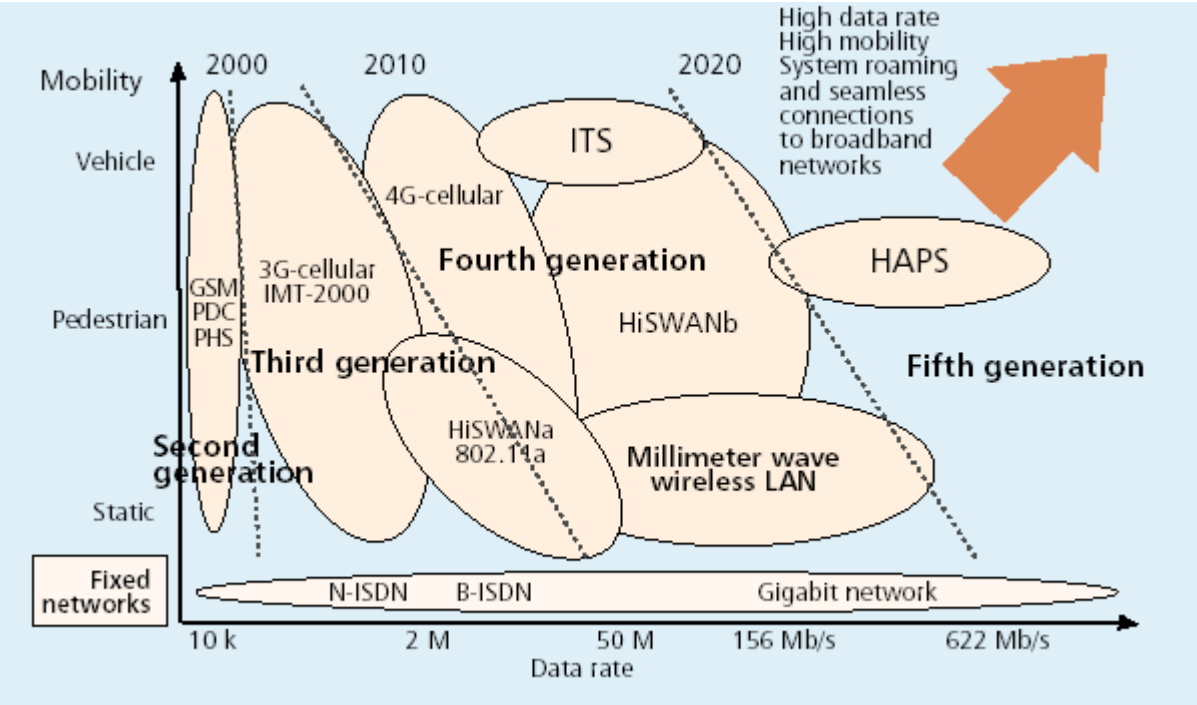
Ob obstoju IPv4 in IPv6 omrežij in mobilnih terminalov so tudi v prehodnem podpornem vozlišču potrebne dostopne točke obeh protokolov kot to prikazuje slika 21. Različne dostopvne točke (izključno IPv4, izključno IPv6, mešane) omogočajo priključitev tako v Internet IPv4 kot Internet IPv6, po potrebi pa tudi tuneliranje s čimer se poenostavijo postopki v mobilnih terminalih.

5. IPv6 IN DOSTOPOVNE TEHNOLOGIJE V OMREŽJIH NASLEDNJE GENERACIJE

V omrežjih naslednje generacije (Next-Generation Networks) bo pomen mobilnosti postajal vse večji, pa naj bo šlo za terminalsko, osebno ali kako drugo mobilnost. Na področju mobilnih tehnologij pričakujemo neke vrste konvergenco oz. zmogljivost terminalov, da podpirajo delovanje v omrežjih različnih tehnologij in omogočajo preklapljanje med njimi na tak način, da uporabnik tega ne zazna.

V današnjih razmerah so na mobilnem področju prevladujoče dostopovne tehnologije celičnih telefonskih sistemov med katerimi še posebej izstopa GSM (Global System fo Mobile communication). Z nadaljnjim razvojem bodo celični sistemi (GPRS, UMTS) svoj primat verjetno obdržali, vendar le do določene mere. Na mestih velike gostote mobilnih terminalov (letališča, nakupovalna središča – t. i. »hot spots«) je pričakovati enostavnejše tehnologije kot npr. brezžična lokalna omrežja (WLAN – Wireless LAN), v pisarnah Bluetooth, DECT ipd. Pri tem gre za ekonomski faktor, saj je npr. omrežje UMTS potrebno zgraditi na novo, poleg tega pa je na mestih velike koncentracije uporaba tehnologije WLAN bistveno enostavnejša in tudi sicer je smiselno integrirati čim več že obstoječih sistemov.

Integracija tehnologij bo postopna, pri tem se običajno navajajo t. i. generacije mobilnih sistemov. Slika 22, povzeta po literaturi [11] prikazuje eno od pojmovanj mobilnih generacij.



slika 22: generacije mobilnih tehnologij (po [11])

V tabeli 1 je naštetih nekaj potencialno uporabnih dostopovnih tehnologij, ki se utegnejo pojaviti v mobilnih omrežjih naslednje generacije.

frekv. delovanja	statična uporaba	pešci	vozila
< 1 GHz			2G, MCA
(1 – 3) GHz	WLAN (802.11b), Bluetooth, WPAN, VSAT	PHS, DECT	2G, 3G, LEO
(3 – 20) GHz	WLAN (802.11a), BRAN, HiSWANa	BRAN, HiSWANa	4G, ITS
(20 – 60) GHz	mm-valovi, HAPS, HiSWANb	HAPS, HiSWANb	ITS, HAPS

2G/3G: mobilni celični sistemi druge in tretje generacije, BRAN: Broadband Radio Access Network, DECT: Digital Enhanced Cordless Telephone, HAPS: High Altitude Platform Station, HiSWAN:High Speed Wireless Access Network, ITS: Intelligent Transportation System, LEO: Low Earth Orbit, MCA: Multi Channel Access, PHS: Personal Handy-phone System, VSAT: Very Small Aperture Terminal, WLAN: Wireless Local Area Network, WPAN: Wireless Personal Area Network.

tabela 1: dostopovne tehnologije

Bistveni problem pri tako široki množici dostopovnih tehnologij je njihova integracija oz. skladno delovanje pri preklapljanju (gostovanju) med njimi. Uporabnik bo imel le en terminal, ki bo moral podpirati večino dostopovnih tehnologij in glede na trenutno lokacijo izbrati najbolj primerno možnost. Mobilni terminal bo imel relativno zapleteno nalogo, saj bo moral pregledati obsežen frekvenčni spekter in izbrati ustrezno tehnologijo dostopa glede na uporabnikove zahteve in možnosti, ki jih je trenutno sposobno zagotoviti omrežje (npr. moč signala). Pri preklapljanju uporabnik ne bo smel čutiti nobenih bistvenih sprememb.

5. 1. UPORABNOST PROTOKOLA IPv6

Glede na vodilno vlogo interneta pri ponudbi storitev v podatkovnih omrežjih in potencialno razširjenostjo mobilnih omrežij je uporaba protokola IPv6 v omrežjih naslednje generacije, kot smo že večkrat poudarili, zelo pričakovana saj bo potrebno praktično vsak mobilni terminal opremiti z javnim IP naslovom.

Pri preklapljanju oz. gostovanju (roaming) v različnih dostopovnih omrežjih se bo večkrat pojavila potreba po spreminjanju IP naslova. Protokol Mobile IP bo v smislu konvergence različnih tehnologij zagotovo upoštevanja vredna rešitev in razlog več za uvajanje protokola IPv6.

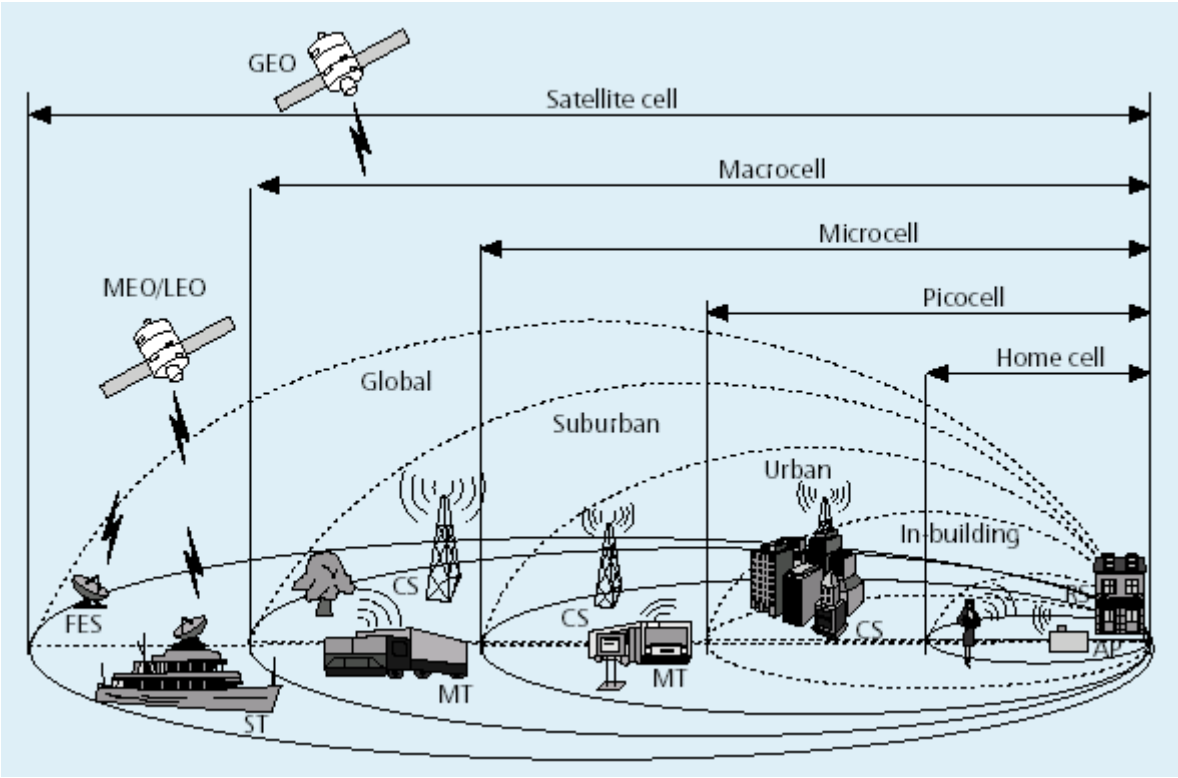
Dobra lastnost protokola IPv6 v smislu konvergenčnosti je tudi rešen problem varnosti – avtentikacije in šifriranja (IPsec – IP security).

5. 2. DELOVANJE HETEROGENEGA MOBILNEGA OMREŽJA

Razvoj globalnega mobilnega in brezžičnega IP omrežja ne bo revolucionaren pač pa precej bolj evolucijski, kar je posledica ekonomskih razlogov, ki želijo čim bolj izkoristiti obstoječo infrastrukturo. Infrastruktura brezžičnega omrežja naslednje generacije bo hierarhična:

- lokalne celice v stanovanjskih in poslovnih objektih ter na javnih površinah (letališča, železniške postaje, konferenčna središča ipd.) temelječe na tehnologijah WLAN, Bluetooth ipd.;
- pikocelice za področje delov naselij: GSM, DECT;
- mikrocelice za pokrivanje naselij in bližnje okolice ter makrocelice na širšem območju: tehnologije celičnih telekomunikacijskih sistemov (GSM, HSCSD, GPRS, UMTS, CDMA);
- satelitske celice za celotno zemeljsko površje pa so obvladljive s satelitskimi sistemi v nizkih (LEO), srednjih (MEO) in geostacionarnih orbitah (GEO).

Opisano hierarhijo prikazuje slika 23 (povzeto po [12]).



slika 23: generacije mobilnih tehnologij (po [12])

Za zagotovitev gostovanja v tako kompleksnem heterogenem omrežju je prvi korak povezljivost na fizičnem nivoju (nivo 1 po OSI modelu). Ločimo dve vrsti predajanja zvez:

- vertikalno (vertical handover): prehod v omrežje druge tehnologije:
- horizontalno (horizontal handover): prehod v drugo celico enake tehnologije.

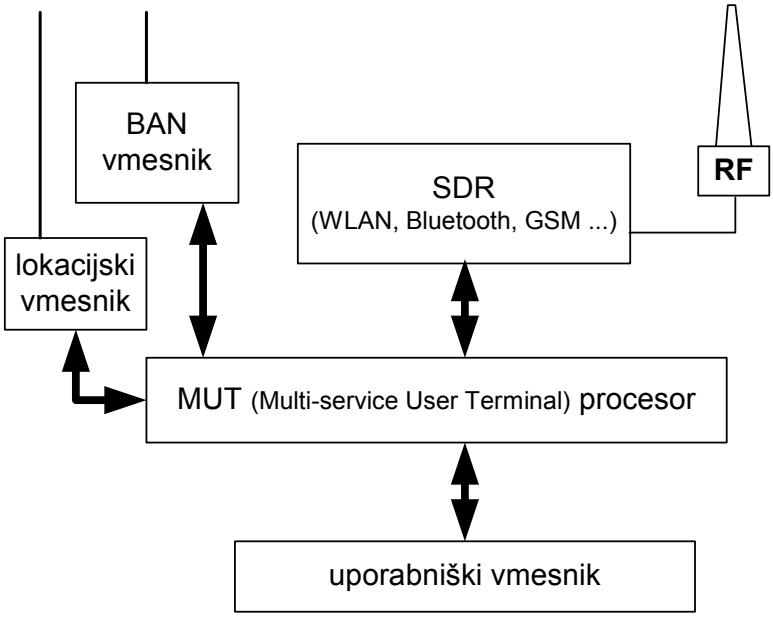
Povezljivost na fizičnem nivoju je zagotovljena s terminalom, ki podpira več različnih tehnologij. Obstaja možnost terminala z več vmesniki ali uporaba tehnologije SDR (Software Defined Radio). Povezljivost na omrežnem nivoju pa je, kot že rečeno, možno zagotoviti s funkcijami mobilnosti protokola IPv6. Uporaba funkcij mobilnosti (protokol Mobile IP) je potrebna, če pri prehodu v omrežje druge dostopovne tehnologije pride do zamenjave IP

naslova mobilnega terminala. Ob zamenjavi omrežja ne pride vedno do zamenjave IP naslova, kar je odvisno od izvedbe omrežja.

Zaradi različnih dostopovnih tehnologij heterogenega omrežja in s tem različnih omrežnih elementov je potrebno zagotoviti skupno jedrno omrežje, ki služi za nemoteno gostovanje uporabnikov in izmenjavo uporabniških (IP) paketov. Da bi povezali različna dostopovna omrežja vsako izmed njih potrebuje povezovalni element – storitveno podporno vozlišče (SSN – Service Support Node). Storitveno vozlišče je hkrati uporabljeno tudi kot strežnik za avtentikacijo, avtorizacijo in tarifiranje. K povezovalnim elementom spadajo še prehodna vozlišča za povezovanje paketno in tokokrogovno komutiranih omrežij (podatkovni prehodi, prehodi za telefonijo).

Gostovanje s horizontalnimi prevzemi (horizontal handover) poteka po običajnih postopkih, ki veljajo za posamezna omrežja. Večjo težavo predstavljajo vertikalni prevzemi kjer je potrebno zamenjati dostopovno tehnologijo. Denimo, da je mobilni terminal prijavljen v omrežje WLAN, nakar se premakne izven dosega omenjenega omrežja v območje omrežja GSM. Terminal mora najprej ugotoviti v katero omrežje se bo preklopil, nato pa lahko začne z mehkim preklapljanjem (soft handover). Za preklop na fizičnem nivoju je potrebno aktivirati omrežne elemente od bazne postaje do mobilnega komutacijskega centra. Ta preklop je za uporabnikov IP promet transparenten, pri čemer lahko pride do zamenjave IP naslova mobilnega terminala. Neprekinjeno delovanje je kljub zamenjavi IP naslova omogočeno z uporabo mobilnih funkcij protokola IPv6 (Mobile IPv6).

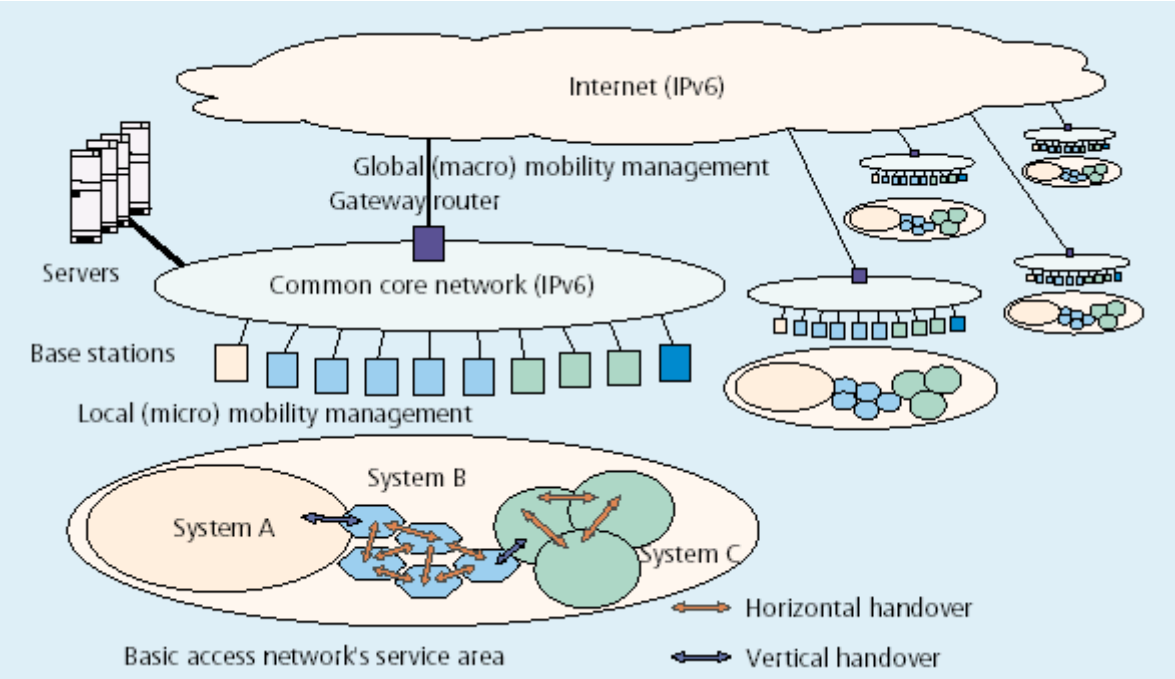
Eno od prihajajočih praktičnih izvedb heterogenega mobilnega omrežja naslednje generacije predstavlja arhitektura MIRAI (Multimedia Integrated network by Radio Access Inovation), ki je del japonskega nacionalnega projekta »e-Japan«. Arhitektura MIRAI predstavlja mobilno omrežje, ki integrira različne dostopovne tehnologije in omogoča povezavo med njimi.



slika 24: MIRAI mobilni terminal

Posebnost je samostojno omrežje (BAN – Basic Access Network), ki skrbi za signalizacijo in optimalno delovanje. V omrežju MIRAI mobilni operater skrbi za svoje jedrno omrežje (Common Core Network), ki združuje več omrežij različnih dostopovnih tehnologij. Ker je nadzor nad jedrnim omrežjem centralen, ima mobilni terminal lahko vedno isti IP naslov vse

dokler se nahaja v istem jedrnem omrežju. Stalna komunikacija z osnovnim dostopovnim omrežjem (BAN) je pomembnaa zlasti zaradi optimizacije, saj je namenjena spremljanju možnih dostopovnih omrežij in hitremu preklapljanju. To dvoje pa zagotavlja dodatno varčevanje z baterijami mobilnega terminala in zmanjšuje možnost, da bi uporabnik občutil zamenjavo dostopovne tehnologije.



slika 25: koncept omrežja MIRAI (po [11])

6. ZAKLJUČEK

Glavna pridobitev ob uvedbi protokola IPv6 v omrežja GPRS in UMTS je povečanje naslovnega prostora, ki omogoča javni IP naslov vsaki mobilni napravi. Potreba po javnih naslovih je predvsem posledica nekaterih specifičnih storitev.

Uvajanje protokola IPv6 bo zagotovo dolgotrajen postopek, ki ga lahko opišemo s tremi fazami prehoda od pretežno IPv4 omrežja, preko mešanega omrežja do pretežno IPv6 omrežja. Pričakujemo lahko, da bodo prav mobilna omrežja med pospeševalci uvajanja protokola IPv6, saj je pomanjkanje IP naslovov izrazito predvsem na nekaterih hitro razvijajočih trgih (npr. Kitajska) mobilne telefonije in mobilnega prenosa podatkov.

Ob uvajanju protokola IPv6 v mobilna omrežja se pojavijo vprašanja o smiselnosti uvajanja. Dokler omrežni elementi kot npr. GGSN ne omogočajo protokola IPv6 tega pravzaprav niti ni možno uvajati. Z uvedbo novega protokola pa v ničemer ne bi bili na slabšem, saj IPv6 naslove s stališča omrežja IPv4 lahko obravnavamo kot zasebne naslove.

7. LITERATURA

[1] J. Wiljakka: Transition to IPv6 in GPRS and WCDMA Mobile Networks; IEEE Communication Magazine, april 2002, str. 134 – 140;

[2] D. G. Waddington, F. Chang: Realizing the Transition to IPv6; IEEE Communications Magazine, junij 2002, str. 138 – 148;

[3] C. E. Perkins: Mobile IP; IEEE Commnunications Magazine; 50th Anniversary Commemorative Issue, maj 2002, str. 66 – 82;

[4] D. B. Johnson, C. E. Perkins, J. Arkko: Mobility Support in IPv6; Internet draft, 18. verzija, junij 2002;

[5] 3GPP TS 23.060 Version 3.8.0 Release 1999; ETSI Technical Specification;

[6] 3GPP TS 03.60 Version 7.7.0 Release 1998; ETSI Technical Specification;

[7] GPRS – How it works, BT CellNet, 2000;

[8] Introducing Mobile IPv6 in 2G and 3G Networks; White Paper, Nokia, 2001;

[9] T. Aljaž: Mobilnost v IPv6; Zbornik 10. delavnice o telekomunikacijah VITEL, Brdo pri Kranju, maj 2000;

[10] S. Tomažič, A. Kos, A. Vugrinec, R. Sušnik: IPv6 internetni protokol naslednje generacije; Laboratorij za komunikacijske naprave, julij 2002;

[11] G. Wu, M. Mizuno, P. J. M. Havinga: MIRAI Architecture for Heterogenous Network; IEEE Communications Magazine, februar 2002, str. 126 – 134;

[12] T. B. Zahariadis, K. G. Vaxevanakis, C. P. Tsantilas, N. A. Zervos, N. A. Nikolau: Global Roaming in Next–Generation Networks; IEEE Communications Magazine, februar 2002, str. 145 – 151.